Syed Irfan Ali Meerza

Ph.D. Candidate @ Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville

(+1) 502-494-8762 | smeerza@vols.utk.edu | irfanmee.github.io

Research Interests

Robust and Trustworthy AI

- Federated Learning
- Machine Unlearning
- Differential Privacy
- Algorithmic Fairness

Responsible Content Governance

- Creative Content Protection
- Generative Model Auditing
- Data Watermarking
- Foundation Model Security

Smart Healthcare and Fitness

- Intelligent Fitness Technologies
- Multimodal Sensing
- Passive Health Tracking
- Early Disease Detection

Education

University of Tennessee, Knoxville — Knoxville, TN
Ph.D. Candidate in Computer Engineering — Aug 2021–May 2026 (expected)
Advisor: Dr. Jian Liu

American International University Bangladesh (AIUB) — Dhaka, Bangladesh
M.Sc. in Electrical and Electronics Engineering (**Gold Medalist**) — Jan 2018–Nov 2019

Khulna University of Engineering and Technology — Khulna, Bangladesh
B.Sc. in Electronics and Communication Engineering — Feb 2011–Jun 2015

Publication

[1] **[IEEE S&P/Oakland, 26] Syed Irfan Ali Meerza**, Jian Liu, "MusicShield: Protection for Musicians in the Era of Generative AI," *Accepted at the 47th IEEE Symposium on Security and Privacy*, **(IEEE S&P)**, 2025. **(Acceptance Rate: 13%)**

[2] **[UbiComp, 25]** Chandler Jackson Bauder, Tianhao Wu, **Syed Irfan Ali Meerza**, Aly Fathy, Jian Liu, "mm-RunAssist: mmWave-based Respiratory and Running Rhythm Analysis During Treadmill Workouts," in *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, **(IMWUT/UbiComp)**, 2025.

[3] **[UbiComp, 25]** Tianhao Wu, Yi Wu, Bibek Poudel, **Syed Irfan Ali Meerza**, Rajasi Gore Athawale, Weizi Li, Zan Gao, Cagdas Karatas, Jian Liu, "VibRun: Real-time Unobtrusive Gait Analysis for Treadmill Running via Footstep Vibrations," in *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, **(IMWUT/UbiComp)**, 2025.

[4] **[PPAI, 25] Syed Irfan Ali Meerza**, Luyang Liu, Jiaxin Zhang, Jian Liu, "GLocalFair: Jointly Improving Global and Local Group Fairness in Federated Learning," in *Proceedings of the 6th AAAI Workshop on Privacy-Preserving Artificial Intelligence*, **(PPAI)**, 2025.

[5] **[IEEE S&P/Oakland, 25] Syed Irfan Ali Meerza**, Lichao Sun, Jian Liu, "HarmonyCloak: Making Music Audio Unlearnable for Generative AI," in *Proceedings of the 46th IEEE Symposium on Security and Privacy*, **(IEEE S&P)**, 2025. **(Acceptance Rate: 14%)**

[6] **[IJCAI, 24] Syed Irfan Ali Meerza**, Jian Liu, "EAB-FL: Exacerbating Algorithmic Bias Through Model Poisoning Attacks in Federated Learning," in *Proceedings of the 33rd International Joint Conference on Artificial Intelligence*, **(IJCAI)**, 2024. **(Acceptance Rate: 14%)**

[7] **[ISVLSI, 24] Syed Irfan Ali Meerza**, Amir Sadovnik, Jian Liu, "ConFUSE: Confusion-based Federated Unlearning with Salience Exploration," in *Proceedings of the IEEE Computer Society Annual Symposium on VLSI*, **(ISVLSI)**, 2024.

[8] **[AsiaCCS, 22]** Yue Cui, **Syed Irfan Ali Meerza**, Zhuohang Li, Luyang Liu, Jiaxin Zhang, Jian Liu, "RecUP-FL: Reconciling Utility and Privacy in Federated Learning via User-configurable Privacy Defense," in *Proceedings of the 18th ACM ASIA Conference on Computer and Communications Security*, **(AsiaCCS)**, 2022. **(Acceptance Rate: 16%)**

[9] **[WNYISPW, 22]** Afsana Ahamed, **Syed Irfan Ali Meerza**, "Iris Recognition Using Curvelet Transform and Accuracy Maximization by Particle Swarm Optimization," in *Proceedings of the IEEE Western New York Image and Signal Processing Workshop*, **(WNYISPW 2022)**, 2022.

[10] **[EMBC, 22] Syed Irfan Ali Meerza**, Zhuohang Li, Luyang Liu, Jiaxin Zhang, Jian Liu, "Fair and Privacy-Preserving Alzheimer's Disease Diagnosis Based on Spontaneous Speech Analysis via Federated Learning," in *Proceedings of the 44th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, **(EMBC)**, 2022.

[11] **[EMBC, 21] Syed Irfan Ali Meerza**, Affan Affan, Hossein Mirinejad, Michael E Brier, Jacek M Zurada, Tamer Inanc, "Precise Warfarin Management Through Personalized Modeling and Control with Limited Clinical Data," in *Proceedings of the 43rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, **(EMBC)**, 2021.

[12] **[AAEA, 21]** Syed Imran Ali Meerza, **Syed Irfan Ali Meerza**, Afsana Ahmed, "Food Insecurity Through Machine Learning Lens: Identifying Vulnerable Households," in *Proceedings of the Agricultural and Applied Economics Association and Western Agricultural Economics Association Joint Annual Meeting*, **(AAEA/WAEA)**, 2021.

[13] **[ICASERT, 19] Syed Irfan Ali Meerza**, Moinul Islam, Md Mohiuddin Uzzal, "Q-Learning Based Particle Swarm Optimization Algorithm for Optimal Path Planning of Swarm of Mobile Robots," in *Proceedings of the IEEE 1st International Conference on Advances in Science, Engineering and Robotics Technology*, **(ICASERT)**, 2019.

[14] **[ICREST, 19] Syed Irfan Ali Meerza**, Moinul Islam, Md Mohiuddin Uzzal, "Performance Evaluation of Different Algorithms for Handwritten Isolated Bangla Character Recognition," in *Proceedings of the 1st International Conference on Robotics, Electrical and Signal Processing Techniques*, **(ICREST)**, 2019.

[15] **[ICITISEE, 18] Syed Irfan Ali Meerza**, Moinul Islam, Md Mohiuddin Uzzal, "Optimal Path Planning Algorithm for Swarm of Robots Using Particle Swarm Optimization Technique," in *Proceedings of the IEEE 3rd Conference on Information Technology, Information Systems and Electrical Engineering*, **(ICITISEE)**, 2018.

Manuscripts

[1] **Syed Irfan Ali Meerza**, Jiawei Yu, Yi Chen Liu, Xi Gua, Jian Liu, "Harmonizing Perception: Human vs. AI Capabilities in Identifying AI-Generated Music," *Submitted to the 35th Usenix Security Symposium*, **(USENIX Security 2026)**, 2026. **(*In review*)**

[2] **Syed Irfan Ali Meerza**, Feiyi Wang, Jian Liu, "FedSpy-LLM: Towards Scalable and Generalizable

Data Reconstruction Attacks from Gradients on LLMs," *Submitted to the 35th Usenix Security Symposium*, **(USENIX Security 2026)**, 2026. **(*In review*)**

[3] **Syed Irfan Ali Meerza**, Oktay Ozturk, Amir Sadovnik, Jian Liu, "DiffUE: Enhancing Utility Unlearnability Trade-offs in Unlearnable Examples Against Relearning with Diffusion Autoencoders," *Submitted to the 40th Annual AAAI Conference on Artificial Intelligence*, **(AAAI 2026)**, 2026. **(*In review*)**

[4] Jiawei Yu, **Syed Irfan Ali Meerza**, Yi Wu, Amir Sadovnik, Jian Liu, "SemPurify: Semantics-Aware Data Purification Against Backdoor Attacks," *Submitted to the 40th Annual AAAI Conference on Artificial Intelligence*, **(AAAI 2026)**, 2026. **(*In review*)**

[5] **Syed Irfan Ali Meerza**, Jian Liu, "MusicTrace: Certifiably Robust, General Purpose Watermarking for Traceability Through Generative Music Models," *Submitted to the IEEE International Conference on Acoustics, Speech, and Signal Processing*, **(ICASSP 2026)**, 2026. **(*In review*)**

Patents

[1] Jian Liu, Syed Irfan Ali Meerza, Lichao Sun, "HarmonyCloak: Making Music Audio Unlearnable for Generative AI," U.S. Provisional Application, April 2025.

[2] Jian Liu, Syed Irfan Ali Meerza, "MusicShield: Protection for Musicians in the Era of Generative AI," U.S. Provisional Application, April 2025.

Awards, Grants and Fellowships

Awards

- "Gonzalez Family Outstanding Graduate Research Assistant," University of Tennessee, Knoxville, 2025
- "Honorable Mention (Team)", MagNet Challenge, Princeton University, New Jersey, USA, 2023
- Received "Chancellor's Award" and "Vice-Chancellor's Award", AIUB, 2020
- Winner (Team) (Khulna Division), Digital Innovation Fair, Bangladesh, 2015
- Top 20 nomination for "Young Bangla Youth Award", Bangladesh, 2015

Grants

- NSF Non-Academic Research Internship for Graduate Students (INTERN) Supplemental Funding ($55,000), 2024
- GSS Travel Grant UTK ($400), 2025
- PPAI Workshop Travel Grant, AAAI Workshop on Privacy-Preserving Artificial Intelligence ($500), 2025
- GSS Travel Grant UTK ($1,150), 2024
- IJCAI Travel Grant, 33rd International Joint Conference on Artificial Intelligence (IJCAI) ($350), 2024

Fellowships

- EERE Fellow, Department of Energy Efficiency and Renewable Energy and University of Tennessee, Knoxville ($10,000), 2022-2023
- Tennessee's Top 100 Fellow, University of Tennessee, Knoxville ($40,000), 2021-2025
- Khulna University of Engineering and Technology Merit Scholarship, 2012-2015

Professional Experience

Graduate Research Intern, Oak Ridge National Laboratory Jan. 2025–May 2025, Oak Ridge, TN
Advisor: Dr. Feiyi Wang May 2024–Aug. 2024, Oak Ridge, TN

- Develop a scalable and generalizable data reconstruction attack from gradients on LLMs in the FedLLM.
- Develop an LLM training protocol to train a proprietary large language model on clinical notes data.
- Designed a communication-efficient FL framework to train an LLM model on heterogeneous communication restricted clients.

Graduate Research Assistant, University of Tennessee Knoxville Aug. 2021 – Present, Knoxville, TN

- Developed methods to ensure privacy, fairness, and unlearning capabilities in distributed and federated learning systems, addressing emerging challenges in algorithmic accountability and personalized data protection.
- Designed techniques to safeguard creative digital content from misuse by generative AI models, focusing on robust watermarking, auditing, and content cloaking to uphold creator rights and data ownership.
- Advanced intelligent fitness and healthcare technologies by integrating AI with multimodal sensor data, enabling unobtrusive, real-time analysis of human activity and physiological signals for improved wellness monitoring.

Executive Engineer, Bashundhara Oil and Gas Company Ltd. Feb 2017–Nov 2019, Dhaka, Bangladesh

- Reviewed electrical and distributed control systems (DCS) for oil refinery and bitumen plants.

Assistant Engineer, R&D, Walton Hi-Tech Industries Ltd. Feb 2016–Aug 2016, Dhaka, Bangladesh

- Designed electronic control systems and algorithms for refrigerators and air conditioners.
- Developed PCB designs for refrigeration and air conditioning systems.

Teaching Experience

Lab Instructor, The University of Tennessee, Knoxville Fall 2025
COSC-102 Introduction to Computer Science
Led weekly labs for **35** students; developed exercises and graded assignments.

Teaching Assistant, The University of Tennessee, Knoxville Fall 2024
ECE-569 Mobile and Embedded System Security
Assisted course delivery for **50** graduate students; held office hours and graded projects.

Guest Lecture, The University of Tennessee, Knoxville Spring 2024
COSC-526 Data Mining and Analytics
Delivered a **60-minute** lecture on data privacy and security; received positive feedback from students and instructor.

Teaching Assistant, The University of Tennessee, Knoxville Spring 2024
COSC-526 Data Mining and Analytics
Supported course for **27** graduate students; assisted with grading, projects, and exam preparation.

Teaching Assistant, The University of Tennessee, Knoxville Fall 2023
COSC-522 Machine Learning
Assisted with lectures and assignments for **45** graduate students; held weekly office hours.

Mentorship and Academic Supervision

Undergraduate Students

- Minjae Bae — UTK EECS, 2024–Current
- Shawn-Patr Barhorst — UTK EECS, 2024–2025
- Maximus Nwider — UTK EECS, 2023–2025
- Luis Gonzalez — UTK EECS, 2021–2023

MS Students

- Xiande Zhang — UTK EECS, 2022–2024
- Oktay Ozturk — UTK EECS, 2023–2024

PhD Students

- Tianhao Wu — UGA SoC, 2023–Current
- Jiawei Yu — UGA SoC, 2024–Current
- Yi Chen Liu — UGA SoC, 2024–Current

Selected Media Mentions

Jul 2025	**how to poison AI music scrapers** — killswitch@kaleidoscope (*Apple Podcast*)
May 2025	**Pitch perfect protection**. *EurekAlert*.
Apr 2025	**The Art Of Poison-Pilling Music Files**. Benn Jordan (*YouTube*, **615k** Views).
Dec 2024	**You can't hear it, but the University of Tennessee tool 'cloaks' songs to protect music from AI**. *Knox News*.
Oct 2024	**Liu's New Tool Makes Songs Unlearnable to Generative AI**. *UTK News*.
Oct 2024	**New Tool Makes Songs Unlearnable to Generative AI**. Featured in *TechXplore*, *Softonic*, *Futura*, *Knowridge*, *New Atlas*, etc.
Oct 2024	**HarmonyCloak slips silent poison into music to corrupt AI copies**. *New Atlas*.
Oct 2024	**Someone has come up with a cloaking device to fight bogus AI music. It's pretty cool**. *Alan Cross' Journal of Musical Things*.
Oct 2024	**HarmonyCloak: A New Tool to Protect Musicians from AI Copyright Infringement**. *The Outpost*.
Oct 2024	**Herramienta dificulta a la IA entrenarse con canciones**. *Tecnología*.
Oct 2024	**New tech makes songs invisible to AI, protecting artists from copycats**. *Knowledge*.

Professional Activities

- Reviewer, IEEE Computer Society Annual Symposium on VLSI (ISVLSI),(2024).
- Reviewer, IEEE Transactions on Network Science and Engineering, (2024).
- Reviewer, ACM SIGKDD Conference on Knowledge Discovery and Data Mining, (2024)
- Mentor, HackUTK student hackathon, University of Tennessee (2022–2023)
- Volunteer, IEEE Computer Society – Bangladesh Chapter (2017–2019)
- Member and Mentor, MEC Robotics Club, Khulna University of Engineering and Technology, Khulna (2012–2015)